

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF TENNESSEE**

**KIM P. WILLIAMS**, *individually and on  
behalf of all others similarly situated*,

**Case No.**

Plaintiff,

**CLASS ACTION COMPLAINT**

v.

**UNUM GROUP**,

**JURY TRIAL DEMANDED**

Defendant.

---

**CLASS ACTION COMPLAINT**

Plaintiff Kim P. Williams, individually and on behalf of all similarly situated persons, alleges the following against Unum Group (“Unum” or “Defendant”) based on personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents, as to all other matters:

**I. INTRODUCTION**

1. Plaintiff brings this class action against Unum for its failure to properly secure and safeguard Plaintiff’s and other similarly situated customers’ sensitive information, including full names, dates of birth, addresses, policy/account numbers, and Social Security numbers (“personally identifiable information” or “Private Information”) and medical and health insurance information, which is protected health information (“PHI,” and collectively with Private Information, “Private Information”) as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

2. Defendant is a Fortune 500 company that owns insurance companies that provide disability, life, accident, critical illness, dental, and vision benefits to employees at 182,000



businesses in the U.S. and U.K.<sup>1</sup>

3. Upon information and belief, former and current customers of Defendant's subsidiary insurance companies are required to entrust Defendant with sensitive, non-public Private Information, without which Defendant's subsidiaries could not perform their regular business activities, in order to obtain services from Defendant's subsidiaries. Defendant retains this information for at least many years and even after the consumer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about June 1, 2023, Defendant learned that an instance of its MOVEit Transfer application was penetrated by a cyberattack.<sup>2</sup> On June 4, 2023, Unum's investigation with the assistance of third-party cybersecurity experts "identified evidence that, between May 31, 2023 and June 1, 2023, an unauthorized party had exploited the security vulnerability to copy data."<sup>3</sup> As a result of its investigation, Defendant concluded—on an undisclosed date—that Plaintiff's and Class Members' Private Information was compromised in the Data Breach.<sup>4</sup>

6. According to an untitled letter sent to Plaintiff and Class Members, on behalf of Defendant (the "Notice Letter"), the compromised Private Information included individuals' names, addresses, dates of birth, Social Security numbers or individual tax identification number, medical information, health insurance claim information and policy information.<sup>5</sup>

7. Defendant failed to adequately protect Plaintiff's and Class Members Private

---

<sup>1</sup> <https://www.unum.com/about> (last visited Aug. 16, 2023).

<sup>2</sup> See Ex. A ("Notice Letter").

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*



Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

10. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.



11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

12. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

## **II. PARTIES**

13. Plaintiff Kim P. Williams, is, and at all times mentioned herein was, an individual citizen and resident of Melbourne, Florida. Plaintiff received a Notice of Data Breach letter (attached hereto as **Exhibit A**), via U.S. mail.<sup>6</sup>

14. Defendant Unum Group is a Delaware corporation with its principal place of business located at 1 Fountain Square, Chattanooga, Tennessee 37402.

## **III. JURISDICTION AND VENUE**

15. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of

---

<sup>6</sup> See Ex. A.



interest and costs. The number of class members is over 100, many of whom reside outside the state of Texas and have different citizenship from Unum, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

16. This Court has jurisdiction over Unum because Unum operates in and is headquartered in this District.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District, a substantial part of the events giving rise to this action occurred in this District, and Unum has harmed Class Members residing in this District.

#### **IV. FACTUAL ALLEGATIONS**

##### **A. *Defendant's Business***

18. Defendant is a Fortune 500 company whose subsidiaries provide “a full array of benefits solutions, including benefits communication, enrollment services and claims support.”<sup>7</sup>

19. Plaintiff and Class Members are current and former customers of Unum’s subsidiary insurance companies.

20. As a condition of receiving its products and/or services, Unum’s subsidiary insurance companies require that their customers, including Plaintiff and Class Members, entrust them with highly sensitive personal information.

21. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

22. Upon information and belief, Defendant and its subsidiaries made promises and

---

<sup>7</sup> <https://www.unum.com/about> (last visited Aug. 16, 2023).



representations to their customers, including Plaintiff and Class Members, that the Private Information collected from them as a condition of obtaining products and/or services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

23. Plaintiff and Class Members provided their Private Information to Defendant's subsidiaries with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

25. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep consumer's Private Information safe and confidential.

26. Defendant had obligations created by FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

27. Defendant derived a substantial economic benefit from collecting Plaintiff's and



Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

**B. *The Data Breach***

29. On or about August 3, 2023, Unum began sending Plaintiff and other Data Breach victims an untitled letter, on behalf of Defendant, (the "Notice Letter"), informing them that:

**What Happened?** On June 1, 2023, Unum detected suspicious activity involving an instance of its MOVEit Transfer application. Unum promptly launched an investigation with the assistance of third-party cybersecurity experts. On June 4, 2023, the investigation identified evidence that, between May 31, 2023 and June 1, 2023, an unauthorized party had exploited the security vulnerability to copy data. On July 22, 2023, Unum learned that records containing your personal information were impacted.

**What Information Was Involved?** The information involved varied by individual and may have included name, date of birth, Social Security number or individual tax identification number, medical information, health insurance claim information, and policy information. Financial information and other government issued identification numbers were involved for a limited number of individuals.<sup>8</sup>

30. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

31. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with

---

<sup>8</sup> Notice Letter.



any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive Private Information.

33. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted Private Information of Plaintiff and Class Members, including their Social Security numbers and other sensitive information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

34. Plaintiff further believes her Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type. Moreover, following the Data Breach, Plaintiff has experienced suspicious spam and believes this be an attempt to secure additional Private Information from her.

***C. Defendant Acquires, Collects, and Stores Plaintiff's and the Class's Private Information.***

35. As a condition to obtain products and/or services from Unum and its subsidiaries, Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Defendant.

36. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class



Members' Private Information, Defendant would be unable to perform its services.

37. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

39. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

40. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

41. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

***E. Defendant Knew or Should Have Known of the Risk Because Financial Institutions in Possession of Private Information Are Particularly Susceptable to Cyber Attacks.***

42. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting financial institutions that collect and store Private Information, like Defendant, preceding the date of the breach.



43. Data thieves regularly target companies like Defendant's due to the highly sensitive information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

44. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.<sup>9</sup>

45. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

46. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems, or those of its vendors, were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

47. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

48. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the

---

<sup>9</sup> See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (<https://notified.idtheftcenter.org/s/>), at 6.



foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

49. Additionally, as companies became more dependent on computer systems to run their business,<sup>10</sup> e.g., working remotely as a result of the COVID-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.<sup>11</sup>

50. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals’ detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

51. In the Notice Letter, Defendant offers to cover identity monitoring services for a period of 24 months. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members’ Private Information. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

52. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members’ sensitive Private Information *was* in fact affected, accessed, compromised, and

---

<sup>10</sup> <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html> (last visited Aug. 16, 2023).

<sup>11</sup> <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022> (last visited Aug. 16, 2023).



exfiltrated from Defendant's computer systems.

53. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

54. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

55. As a financial institution in possession of its customers' and former customers' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

#### **F. *Value Of Personally Identifiable Information***

56. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>12</sup> The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number,

---

<sup>12</sup> 17 C.F.R. § 248.201 (2013).



employer or taxpayer identification number.”<sup>13</sup>

57. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.<sup>14</sup>

58. For example, PII can be sold at a price ranging from \$40 to \$200.<sup>15</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>16</sup>

59. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—names and Social Security numbers.

60. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”<sup>17</sup>

61. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

62. The fraudulent activity resulting from the Data Breach may not come to light for

---

<sup>13</sup> *Id.*

<sup>14</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, DIGITAL TRENDS, Oct. 16, 2019, <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Aug. 16, 2023).

<sup>15</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Aug. 16, 2023).

<sup>16</sup> *In the Dark*, VPNOVERVIEW, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Aug. 16, 2023).

<sup>17</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Aug. 16, 2023).



years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>18</sup>

**G. *Unum Failed to Comply with FTC Guidelines.***

63. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

64. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating

---

<sup>18</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Aug. 16, 2023).



someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

65. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. These FTC enforcement actions include actions against financial institutions, like Defendant.

68. As evidenced by the Data Breach, Unum failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Unum's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

69. Unum was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.



**H. Defendant Fails to Comply with HIPAA Guidelines.**

1. Defendant is a covered Business Associate under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

2. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").<sup>19</sup> See 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

3. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

4. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

5. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

6. "Electronic protected health information" is "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

7. HIPAA's Security Rule requires Defendant to do the following:

---

<sup>19</sup> HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.



a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

8. HIPAA also requires Defendant to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

9. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.



10. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and *in no case later than 60 days following discovery of the breach.*"<sup>20</sup>

11. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

12. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

13. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.<sup>21</sup> The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good

---

<sup>20</sup> Breach Notification Rule, U.S. Dep't of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added) (last visited Aug. 16, 2023).

<sup>21</sup> <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last visited Aug. 16, 2023).



business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.<sup>22</sup>

**I. *Unum Failed to Comply with Industry Standards.***

70. As noted above, experts studying cybersecurity routinely identify financial institutions as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

71. Some industry best practices that should be implemented by financial institutions dealing with sensitive Private Information, like Unum, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

72. Other best cybersecurity practices that are standard in the financial industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

73. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

---

<sup>22</sup> <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last visited Aug. 16, 2023).



PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

74. Defendant failed to comply with these accepted standards in the financial industry, thereby permitting the Data Breach to occur.

**J. *Unum Breached Its Duty to Safeguard Plaintiff's and Class Members' Private Information.***

75. In addition to its obligations under federal and state laws, Unum owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Unum owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

76. Unum breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Unum's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect customers' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to audit, monitor, or ensure the integrity of its vendor's data security



practices;

- e. Failing to sufficiently train its employees and vendors regarding the proper handling of its customers Private Information;
- f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- g. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and
- h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

77. Unum negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

78. Had Unum remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

#### **J. *Common Injuries & Damages***

79. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the



materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

**K.        *The Data Breach Increases Victims' Risk of Identity Theft.***

80.        Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

81.        The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

82.        The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

83.        Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

84.        For example, armed with just a name and date of birth, a data thief can utilize a



hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

85. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.<sup>23</sup>

86. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

87. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not

---

<sup>23</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm> (last visited Aug. 16, 2023).



be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

88. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

89. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

90. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

**L. *Loss Of Time to Mitigate Risk of Identity Theft and Fraud***

91. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

92. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice Letter instructs, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

93. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result



of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and resecuring their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

94. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>24</sup>

95. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>25</sup>

96. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:<sup>26</sup>

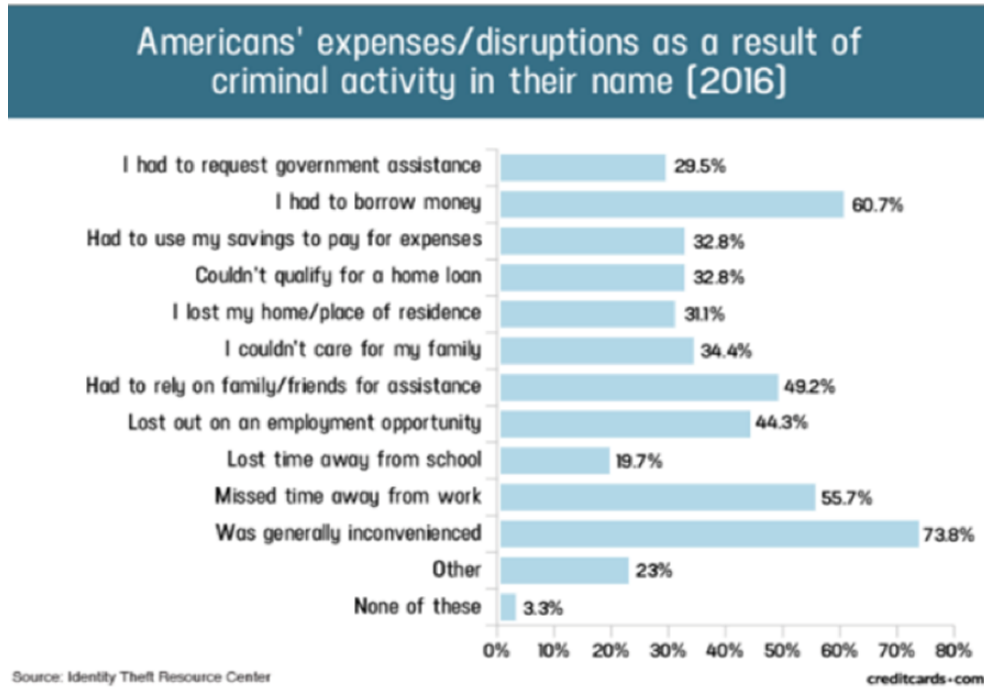
---

<sup>24</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

<sup>25</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited Aug. 16, 2023).

<sup>26</sup> Jason Steele, “Credit Card and ID Theft Statistics,” Oct. 24, 2017, <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Aug. 16, 2023).





97. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>27</sup>

**M. *Diminution in Value of Private Information***

98. Private Information is a valuable property right.<sup>28</sup> Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

<sup>27</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” at 2, U.S. GOV’T ACCOUNTABILITY OFFICE, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Aug. 16, 2023) (“GAO Report”).

<sup>28</sup> See, e.g., Randall T. Soma, et al., Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets, 15 RICH. J.L. & TECH. 11, at \*3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).



99. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>29</sup>

100. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.<sup>30,31</sup>

101. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>32</sup>

102. Conversely sensitive Private Information can sell for as much as \$363 per record on the dark web according to the Infosec Institute.<sup>33</sup>

103. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

104. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to

---

<sup>29</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last visited Aug. 16, 2023).

<sup>30</sup> <https://datacoup.com/> (last visited Aug. 16, 2023).

<sup>31</sup> <https://digi.me/what-is-digime/> (last visited Aug. 16, 2023).

<sup>32</sup> Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last visited Aug. 16, 2023).

<sup>33</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Aug. 16, 2023).



change, *e.g.*, names and Social Security numbers.

105. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

106. The fraudulent activity resulting from the Data Breach may not come to light for years.

107. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

108. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

109. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

**N. *Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.***

110. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make



purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

111. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

112. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

113. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

**O. *Loss of the Benefit of the Bargain***

114. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.



**P. *Plaintiff Williams's Experience***

115. Plaintiff Kim P. Williams is a current customer of one of Unum's subsidiaries.

116. In order to obtain insurance and/or other services at one of Unum's subsidiaries, Plaintiff was required to provide her Private Information to Defendant, including her name, address, date of birth, Social Security number, medical information, health insurance claim information, and policy information.

117. At the time of the Data Breach—approximately May 31, 2023, through June 1, 2023—Defendant retained Plaintiff's Private Information in its system.

118. Plaintiff Williams is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

119. Plaintiff received the Notice Letter, by U.S. mail, from Unum, dated August 3, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her name, date of birth, address, medical information, health insurance claim information, and policy information.

120. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including contacting credit bureaus to place freezes on her accounts; changing passwords and resecuring her own computer network; and checking her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not



limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

121. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) lost or diminished value of her Private Information; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

122. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach and only began following the Data Breach.

123. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

124. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

125. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

126. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.



## V. CLASS ACTION ALLEGATIONS

127. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

128. Specifically, Plaintiff proposes the following class definition, subject to amendment as appropriate:

All individuals in the United States whose Private Information was disclosed in the Data Breach (the “Class”).

129. Excluded from the Class and Subclass are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

130. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or Florida Subclass, as well as add subclasses, before the Court determines whether certification is appropriate.

131. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

132. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes thousands of individuals who have been damaged by Defendant’s conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant’s records.

133. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:



- a. Whether Unum engaged in the conduct alleged herein;
- b. Whether Unum's conduct violated the FTCA and/or HIPAA;
- c. When Unum learned of the Data Breach;
- d. Whether Unum's response to the Data Breach was adequate;
- e. Whether Unum unlawfully shared, lost, or disclosed Plaintiff's and Class Members' Private Information;
- f. Whether Unum failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- g. Whether Unum's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether Unum's data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether Unum owed a duty to Class Members to safeguard their Private Information;
- j. Whether Unum breached its duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members' Private Information via the Data Breach;
- l. Whether Unum had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- m. Whether Unum breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;



- n. Whether Unum knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiff and Class Members suffered as a result of Unum's misconduct;
- p. Whether Unum's conduct was negligent;
- q. Whether Unum was unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

134. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Unum. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

135. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.



136. Predominance. Unum has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Unum's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

137. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Unum. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

138. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Unum has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

139. Finally, all members of the proposed Class are readily ascertainable. Unum has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data



Breach by Unum.

## **CLAIMS FOR RELIEF**

### **COUNT I**

#### **Negligence and Negligence Per Se (*On Behalf of Plaintiff and the Class*)**

140. Plaintiff restates and realleges paragraphs 1 through 139 above as if fully set forth herein.

141. Defendant's subsidiaries require their customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its financial services.

142. Defendant and subsidiaries gathered and stored the Private Information of Plaintiff and Class Members as part of their business of soliciting its services to its clients and its clients' customers, which solicitations and services affect commerce.

143. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

144. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

145. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.



146. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

147. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

148. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

149. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Unum and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Unum with their confidential Private Information, a necessary part of being customers of Defendant.

150. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

151. Defendant was subject to an “independent duty,” untethered to any contract between Defendant and Plaintiff or the Class.



152. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' Private Information it was no longer required to retain pursuant to regulations.

153. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

154. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

155. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;



- f. Failing to remove former customers' Private Information it was no longer required to retain pursuant to regulations; and
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

156. Defendant violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

157. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

158. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes negligence per se.

159. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

160. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

161. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach



of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial industry.

162. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

163. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

164. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

165. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

166. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

167. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

168. Defendant has admitted that the Private Information of Plaintiff and the Class



was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

169. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

170. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

171. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

172. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.



173. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

174. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

175. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

176. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**COUNT II**  
**Breach Of Implied Contract**  
***(On Behalf of Plaintiff and the Class)***

177. Plaintiff restates and realleges paragraphs 1 through 139 above as if fully set forth herein.

178. Plaintiff and Class Members were required to provide their Private Information to Defendant, through its subsidiaries, as a condition of receiving insurance, financial, and/or other services from Defendant and its subsidiaries.

179. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and



confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

180. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

181. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

182. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

183. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

184. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

185. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class



Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

186. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

187. Plaintiff and Class Members paid money and provided their Private Information to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

188. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

189. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

190. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

191. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

192. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.



193. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

194. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT III**  
**Unjust Enrichment**  
***(On Behalf of Plaintiff and the Class)***

195. Plaintiff restates and realleges paragraphs 1 through 139 above as if fully set forth herein.

196. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant's subsidiaries and/or their agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

197. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

198. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

199. Defendant acquired the Private Information through inequitable record retention



as it failed to disclose the inadequate data security practices previously alleged.

200. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Defendant or obtained services at Defendant.

201. Plaintiff and Class Members have no adequate remedy at law for these categories of their damages.

202. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

203. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

204. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.



205. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and Subclass, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
  - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;



- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;



- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;



- xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
  - xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
  - xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;
  - E. For an award of punitive damages, as allowable by law;
  - F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;
  - G. Pre- and post-judgment interest on any amounts awarded; and
  - H. Such other and further relief as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all issues so triable.

Dated: August 17, 2023.



Respectfully submitted,

/s/ Andrew Shamis

Andrew J. Shamis  
**SHAMIS & GENTILE, P.A.**  
14 NE 1st Avenue, Suite 400  
Miami, FL 33132  
Telephone: 305-479-2299  
ashamis@shamisgentile.com

*Counsel for Plaintiff and the Proposed Class*